

**(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)**

**(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international**



(43) Date de la publication internationale
10 juillet 2003 (10.07.2003)

PCT

(10) Numéro de publication internationale

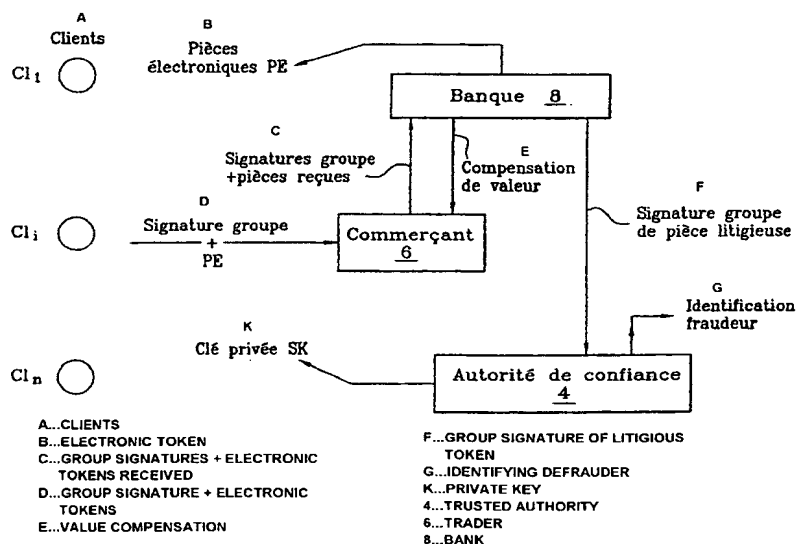
WO 03/056750 A2

- | | |
|---|---|
| <p>(51) Classification internationale des brevets⁷ : H04L 9/32</p> <p>(21) Numéro de la demande internationale :
PCT/FR02/04502</p> <p>(22) Date de dépôt international :
20 décembre 2002 (20.12.2002)</p> <p>(25) Langue de dépôt : français</p> <p>(26) Langue de publication : français</p> <p>(30) Données relatives à la priorité :
01/16950 27 décembre 2001 (27.12.2001) FR</p> <p>(71) Déposant (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,
F-75015 Paris (FR).</p> | <p>(72) Inventeurs; et</p> <p>(75) Inventeurs/Déposants (pour US seulement) : ARDITTI MODIANO, David [FR/FR]; 46ter, rue Paul Vaillant-couturier, F-92140 Clamart (FR). CANARD, Sébastien [FR/FR]; 4, résidence Olympia, F-14000 Caen (FR). GIRAULT, Marc [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). TRAORE, Jacques [FR/FR]; 14, rue Emile Dron, F-81100 Flers (FR).</p> <p>(74) Mandataires : SOMNIER, Jean-Louis etc.; Cabinet Ballot, 122, rue Edouard Vaillant, F-92593 Levallois-Perret Cedex (FR).</p> <p>(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,</p> |
|---|---|

[Suite sur la page suivante]

(54) Title: CRYPTOGRAPHIC SYSTEM FOR GROUP SIGNATURE

(54) Titre : SYSTEME CRYPTOGRAPHIQUE DE SIGNATURE DE GROUPE



(57) Abstract: The invention concerns a system enabling a member (M) of a group (G) to produce, by means of customized data (z; K), a message (m) accompanied by a signature (8) proving to a verifier that the message originates from a member of the group (G). The invention is characterized in that the customized data is in the form of an electronic physical medium (26). Advantageously, the latter also incorporates: encrypting means (B3) for producing a customized cipher (C) from the customized data prior to the signature S of the message (m), means (B5) for producing a combination of a message m to be signed and the cipher (C) associated with said message, for example in the form of a concatenation of the message (m) with the cipher (C), and means (B6) for signing (Sig) the message (m) with the customized data (z; K) in the form of a cipher (C) associated with said message. Advantageously, the physical medium is a smart card (26) or the like.

[Suite sur la page suivante]



WO 03/056750 A2